CISCO 200-201

Cisco CyberOps Associate Certification Questions & Answers

Exam Summary – Syllabus – Questions

200-201

Cisco Certified CyberOps Associate

95-105 Questions Exam – Variable (750-850 / 1000 Approx.)% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your 200-201 Certification Well:

The 200-201 is best suitable for candidates who want to gain knowledge in the Cisco CyberOps. Before you start your 200-201 preparation you may struggle to get all the crucial CyberOps Associate materials like 200-201 syllabus, sample questions, study guide.

But don't worry the 200-201 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the 200-201 syllabus?
- How many questions are there in the 200-201 exam?
- Which Practice test would help me to pass the 200-201 exam at the first attempt?

Passing the 200-201 exam makes you Cisco Certified CyberOps Associate. Having the CyberOps Associate certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Cisco 200-201 CyberOps Associate Certification Details:

Exam Name	Threat Hunting and Defending using Cisco Technologies for CyberOps
Exam Code	200-201
Exam Price	$300 USD
Duration	120 minutes
Number of Questions	95-105
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	**Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)**
Exam Registration	**PEARSON VUE**
Sample Questions	**Cisco 200-201 Sample Questions**
Practice Exam	**Cisco Certified CyberOps Associate Practice Test**

200-201 Syllabus:

Section	Weight	Objectives
Security Concepts	20%	1. Describe the CIA triad 2. Compare security deployments Network, endpoint, and application security systems Agentless and agent-based protections Legacy antivirus and antimalware SIEM, SOAR, and log management 3. Describe security terms Threat intelligence (TI) Threat hunting Malware analysis Threat actor Run book automation (RBA) Reverse engineering Sliding window anomaly detection Principle of least privilege Zero trust Threat intelligence platform (TIP) 4. Compare security concepts Risk (risk scoring/risk weighting, risk reduction, risk assessment) Threat Vulnerability Exploit 5. Describe the principles of the defense-in-depth strategy 6. Compare access control models Discretionary access control Mandatory access control Nondiscretionary access control Authentication, authorization, accounting Rule-based access control Time-based access control

Section	Weight	Objectives
		Role-based access control 7. Describe terms as defined in CVSS Attack vector Attack complexity Privileges required User interaction Scope 8. Identify the challenges of data visibility (network, host, and cloud) in detection 9. Identify potential data loss from provided traffic profiles 10. Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs 11. Compare rule-based detection vs. behavioral and statistical detection
Security Monitoring	25%	1. Compare attack surface and vulnerability 2. Identify the types of data provided by these technologies TCP dump NetFlow Next-gen firewall Traditional stateful firewall Application visibility and control Web content filtering Email content filtering 3. Describe the impact of these technologies on data visibility Access control list NAT/PAT Tunneling TOR Encryption P2P Encapsulation Load balancing

Section	Weight	Objectives
		4. Describe the uses of these data types in security monitoring Full packet capture Session data Transaction data Statistical data Metadata Alert data 5. Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 6. Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 7. Describe social engineering attacks 8. Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 9. Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies 10. Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric) 11. Identify the certificate components in a given scenario Cipher-suite X.509 certificates Key exchange Protocol version PKCS
Host-Based Analysis	20%	1. Describe the functionality of these endpoint technologies in regard to security monitoring Host-based intrusion detection Antimalware and antivirus Host-based firewall Application-level listing/block listing Systems-based sandboxing (such as Chrome, Java, Adobe Reader)

Section	Weight	Objectives
		2. Identify components of an operating system (such as Windows and Linux) in a given scenario 3. Describe the role of attribution in an investigation Assets Threat actor Indicators of compromise Indicators of attack Chain of custody 4. Identify type of evidence used based on provided logs Best evidence Corroborative evidence Indirect evidence 5. Compare tampered and untampered disk image 6. Interpret operating system, application, or command line logs to identify an event 7. Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox) Hashes URLs Systems, events, and networking
Network Intrusion Analysis	20%	1. Map the provided events to source technologies IDS/IPS Firewall Network application control Proxy logs Antivirus Transaction data (NetFlow) 2. Compare impact and no impact for these items False positive False negative True positive True negative

Section	Weight	Objectives
		Benign 3. Compare deep packet inspection with packet filtering and stateful firewall operation 4. Compare inline traffic interrogation and taps or traffic monitoring 5. Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic 6. Extract files from a TCP stream when given a PCAP file and Wireshark 7. Identify key elements in an intrusion from a given PCAP file Source address Destination address Source port Destination port Protocols Payloads 8. Interpret the fields in protocol headers as related to intrusion analysis Ethernet frame IPv4 IPv6 TCP UDP ICMP DNS SMTP/POP3/IMAP HTTP/HTTPS/HTTP2 ARP 9. Interpret common artifact elements from an event to identify an alert IP address (source / destination) Client and server port identity Process (file or registry)

Section	Weight	Objectives
		System (API calls) Hashes URI / URL 10. Interpret basic regular expressions
Security Policies and Procedures	15%	1. Describe management concepts Asset management Configuration management Mobile device management Patch management Vulnerability management 2. Describe the elements in an incident response plan as stated in NIST.SP800-61 3. Apply the incident handling process (such as NIST.SP800-61) to an event 4. Map elements to these steps of analysis based on the NIST.SP800-61 Preparation Detection and analysis Containment, eradication, and recovery Post-incident analysis (lessons learned) 5. Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800-61) Preparation Detection and analysis Containment, eradication, and recovery Post-incident analysis (lessons learned) 6. Describe concepts as documented in NIST.SP800-86 Evidence collection order Data integrity Data preservation Volatile data collection 7. Identify these elements used for network profiling

Section	Weight	Objectives
		Total throughput Session duration Ports used Critical asset address space 8. Identify these elements used for server profiling Listening ports Logged in users/service accounts Running processes Running tasks Applications 9. Identify protected data in a network PII PSI PHI Intellectual property 10. Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion 11. Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

Cisco 200-201 Sample Questions:

Question: 1

When the facility has a fence, guards, a locked front door and locked interior doors, it called what?

a) AUP
b) separation of duties
c) defense in depth
d) piggybacking

Answer: c

Question: 2

You are assessing application or service availability with a port scan. All services use default ports. This is an example of what type of exploit analysis?

a) deterministic
b) predictive
c) probabilistic
d) intuitive

Answer: a

Question: 3

What are two differences in how tampered and untampered disk images affect a security incident?

(Choose two.)

a) Untampered images are used in the security investigation process
b) Tampered images are used in the security investigation process
c) The image is tampered if the stored hash and the computed hash match
d) Tampered images are used in the incident recovery process
e) The image is untampered if the stored hash and the computed hash match

Answer: b, e

Question: 4

Which of the following CVSS scores measures the extent to which the information resource can be changed due to an attack?

a) Availability
b) Confidentiality
c) Integrity
d) Attack vector

Answer: c

Question: 5

An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

a) data from a CD copied using Mac-based system
b) data from a CD copied using Linux system
c) data from a DVD copied using Windows system
d) data from a CD copied using Windows

Answer: b

Question: 6

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

a) encapsulation
b) TOR
c) tunneling
d) NAT

Answer: d

Question: 7

Cisco Active Threat Analysis is an example of which of the following?

a) MSSP
b) PSIRT
c) Coordination centers

d) National CSIRT

Answer: a

Question: 8

A user received a malicious attachment but did not run it. Which category classifies the intrusion?

a) weaponization
b) reconnaissance
c) installation
d) delivery

Answer: d

Question: 9

When TCP packet is sent to an open port with the SYN flag set, what response would be expected from the open port?

a) a packet with the SYN and ACK flags set
b) a packet with an RST flag
c) no response
d) a packet with the ACK flag set

Answer: a

Question: 10

How does an attacker observe network traffic exchanged between two users?

a) port scanning
b) man-in-the-middle
c) command injection
d) denial of service

Answer: b

Study Guide to Crack Cisco CyberOps Associate 200-201 Exam:

- Getting details of the 200-201 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 200-201 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Cisco provided training for 200-201 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 200-201 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 200-201 practice tests is must. Continuous practice will make you an expert in all syllabus areas.